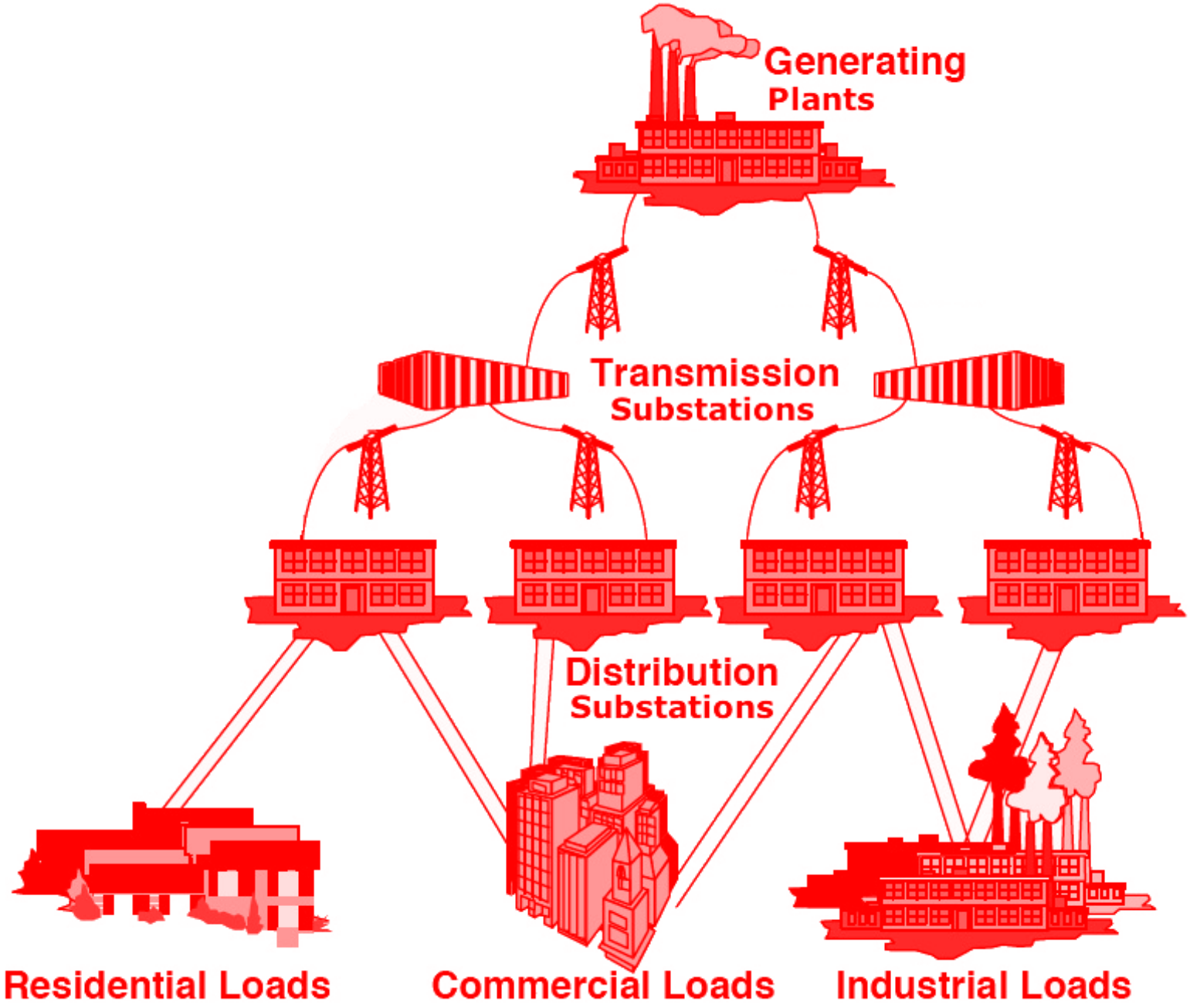
Critical Infrastructures Security Modeling, Enforcement and Runtime Checking

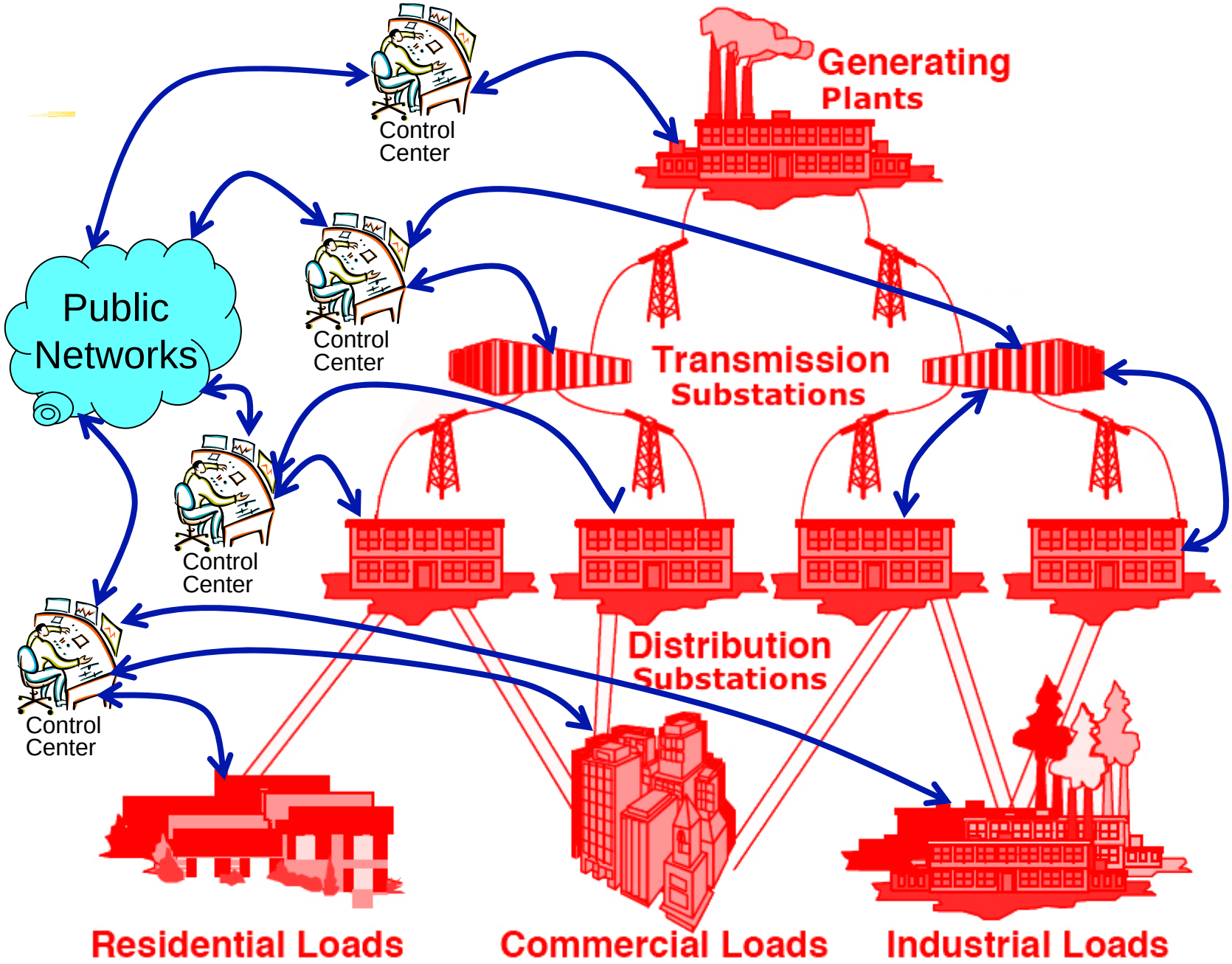
Anas Abou El Kalam, Yves Deswarte
anas.abouelkalam@enseeiht.fr, yves.deswarte@laas.fr

LAAS-CNRS, Toulouse, France

Context: Electrical Power Grid in Europe

- Production, transport, distribution of electrical energy
  - The CRUTIAL european project
    CRitical **UT**ility Infrastrur**AL** resilience.
- Many stakeholders
  - of different **size** (from multinational companies to individual customers),
  - with different **functions** (production, transport, distribution, marketing, brokerage, regulation authorities, …)
  - Most participating companies are competing with each others
- Large (extensible) structures, over large geographic areas and countries
- Information Systems:
  heterogeneous, complex, dynamic, evolvable


Generating
Plants
Transmission
Substations
Distribution
Substations
Residential Loads
Commercial Loads
Industrial Loads


Control Center
Generating Plants
Public Networks
Control Center
Transmission Substations
Control Center
Distribution Substations
Control Center
Residential Loads
Commercial Loads
Industrial Loads

Problem Statement

To address the growing needs of the deregulated market

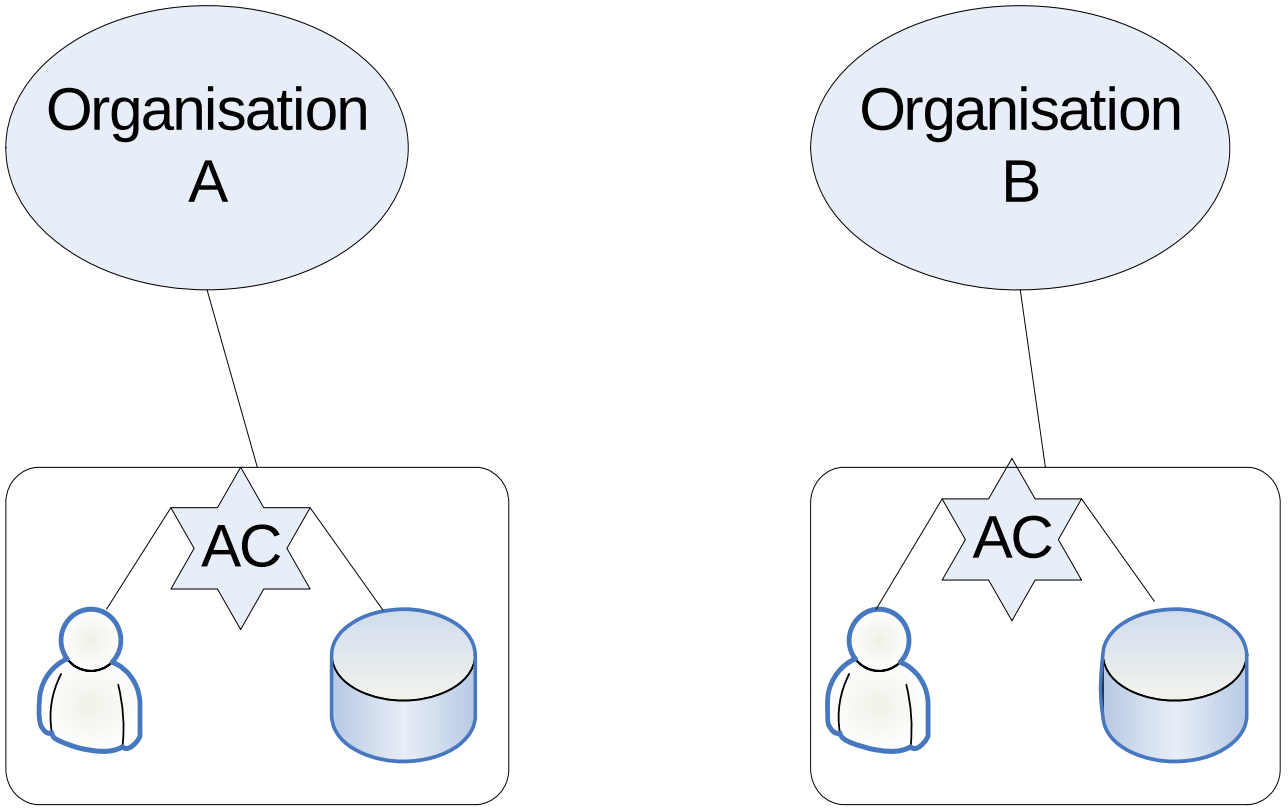
- The different organizations need to share and exchange data and services through public/private networks
  - Security
- They have conflicting interests
  - Mutual suspicion
- They want to keep control and privacy over their own resources, and they are liable of their own employees
  - Autonomy for authentication and authorization

- PolyOrBAC (cf. paper at CIP 2008)
  - Each organization has its own security policy: OrBAC
  - Interaction between organizations through Web Services

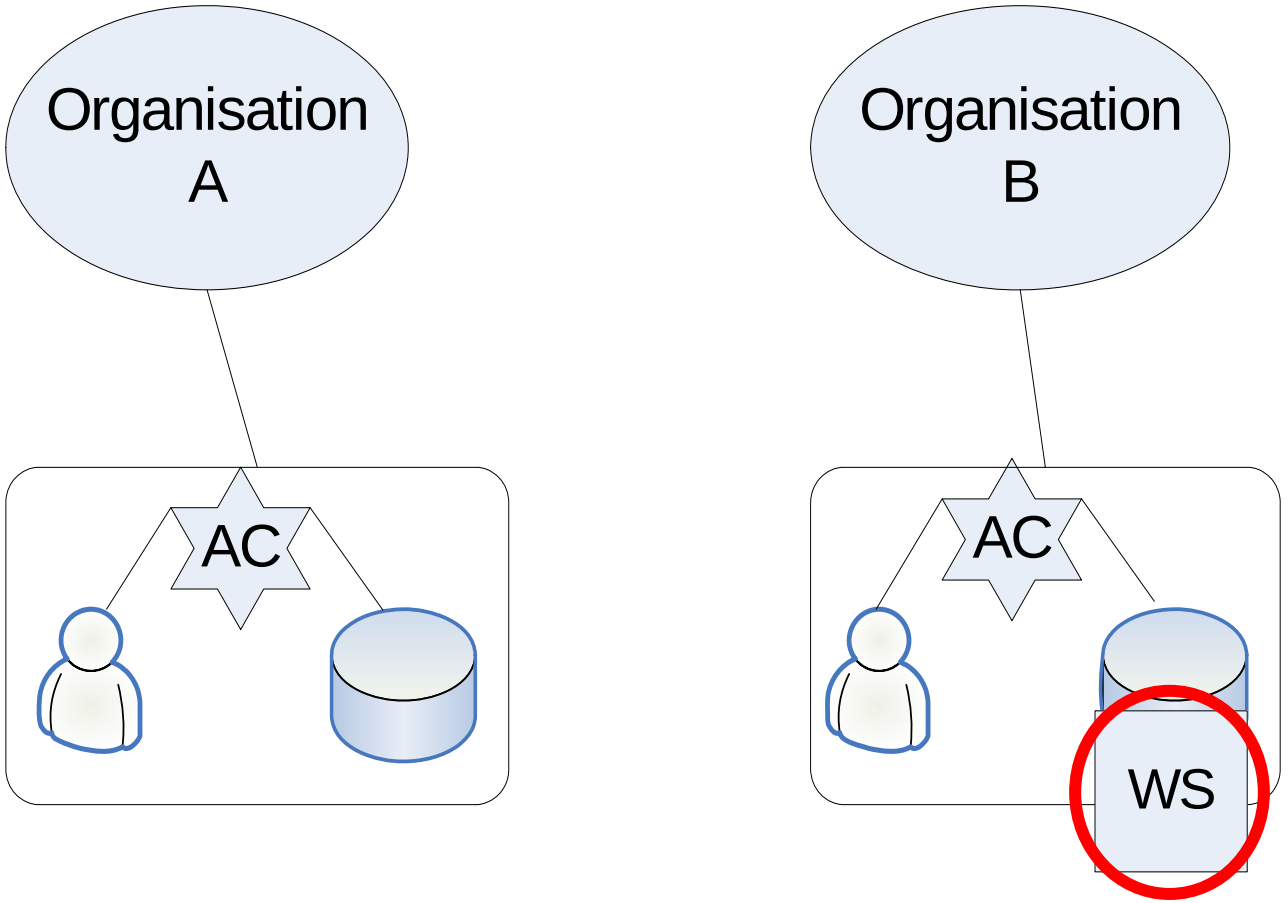
Web Services

- Based on open, standardized, well-known mechanisms and protocols
- WS support **interoperability** between software components belonging to heterogeneous platforms
- **Compatibility** with OrBAC
  - For the organization offering a WS: the other organization is seen as a "virtual user", which plays a role authorized to execute the service
  - For the organization requesting a WS: the WS is seen as an "external object": WS image
  - Authentication & access control within each organization (OrBAC)
  - WS security enforcement: through "contracts"

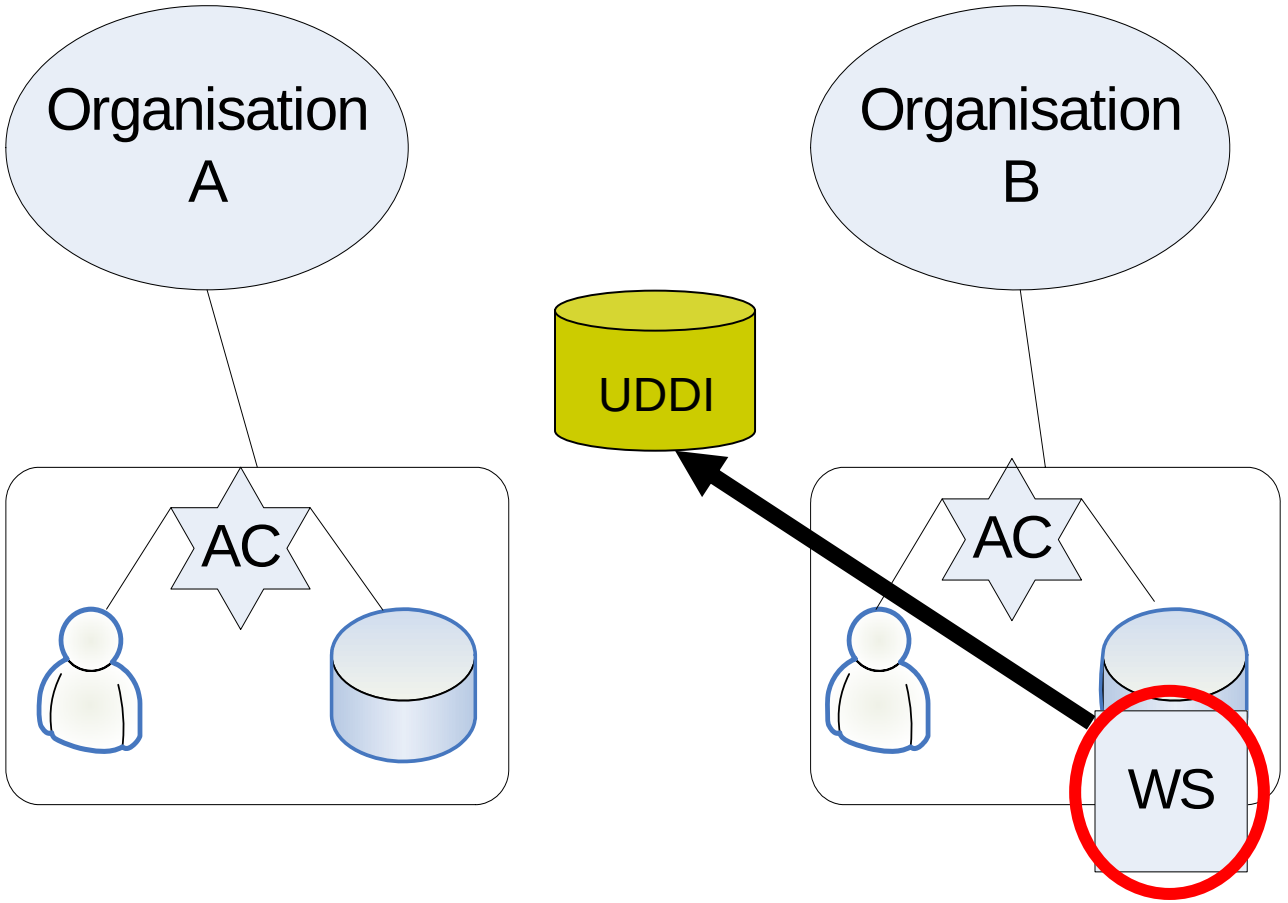
PolyOrBAC & WS



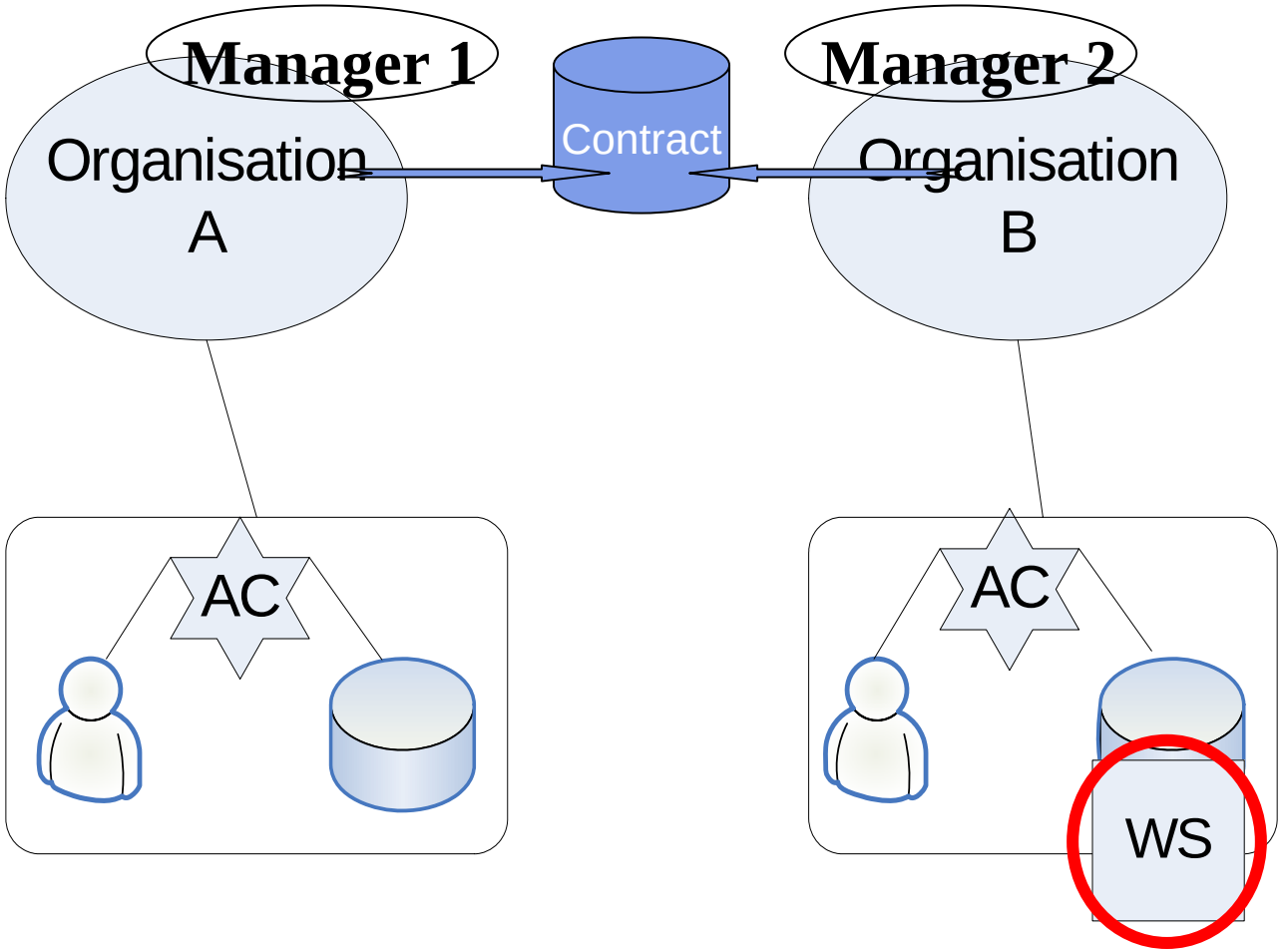
PolyOrBAC & WS



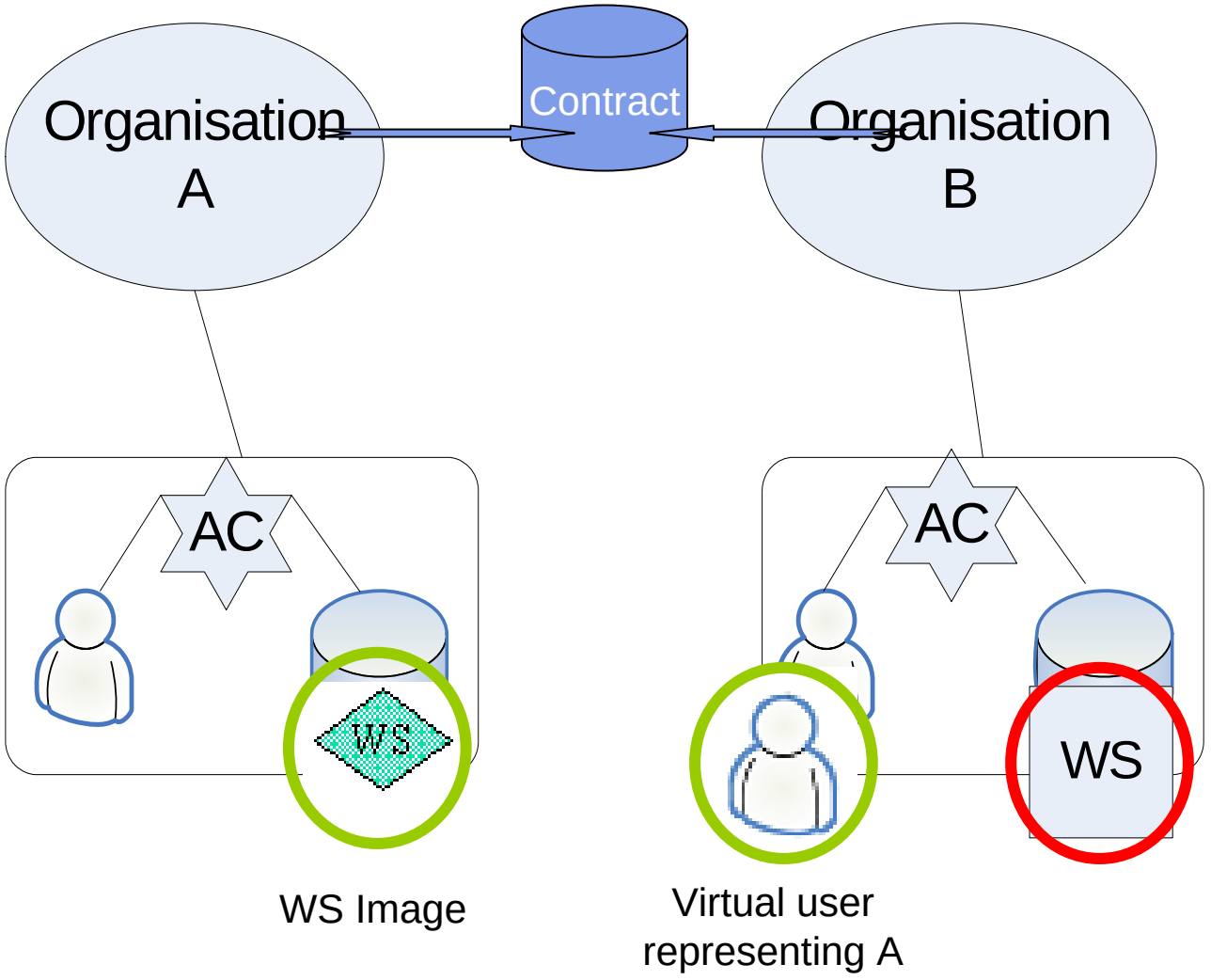
PolyOrBAC & WS



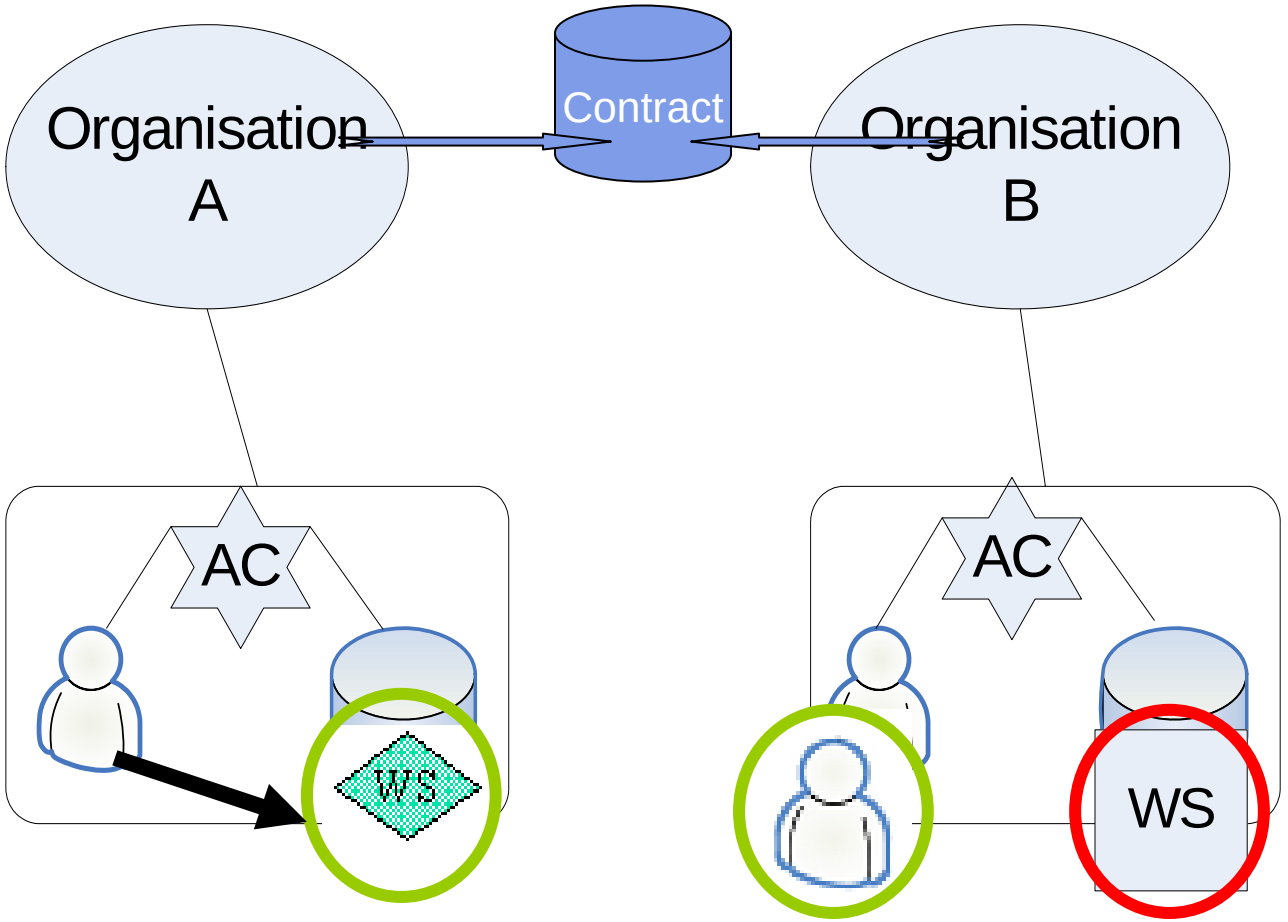
PolyOrBAC & WS



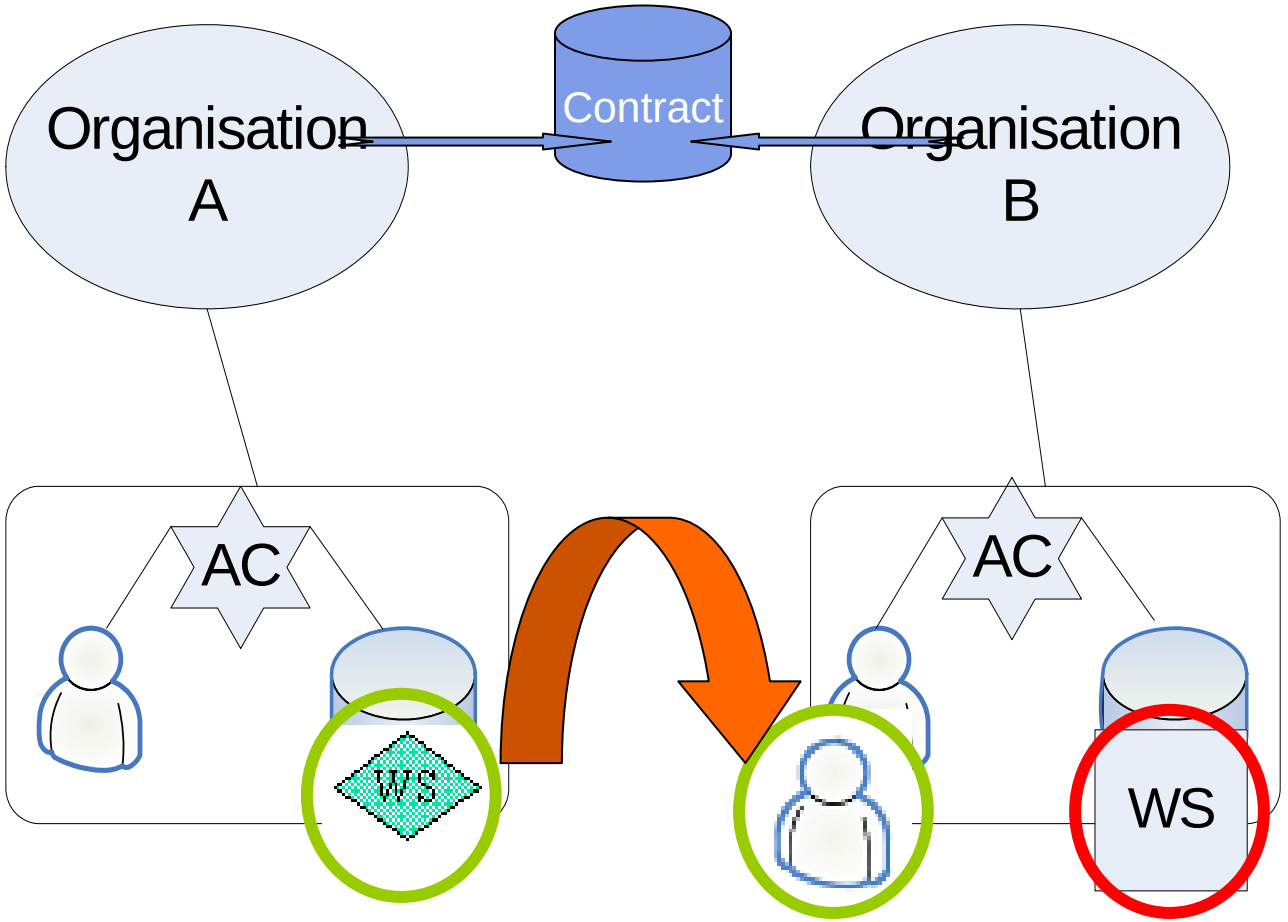
PolyOrBAC & WS



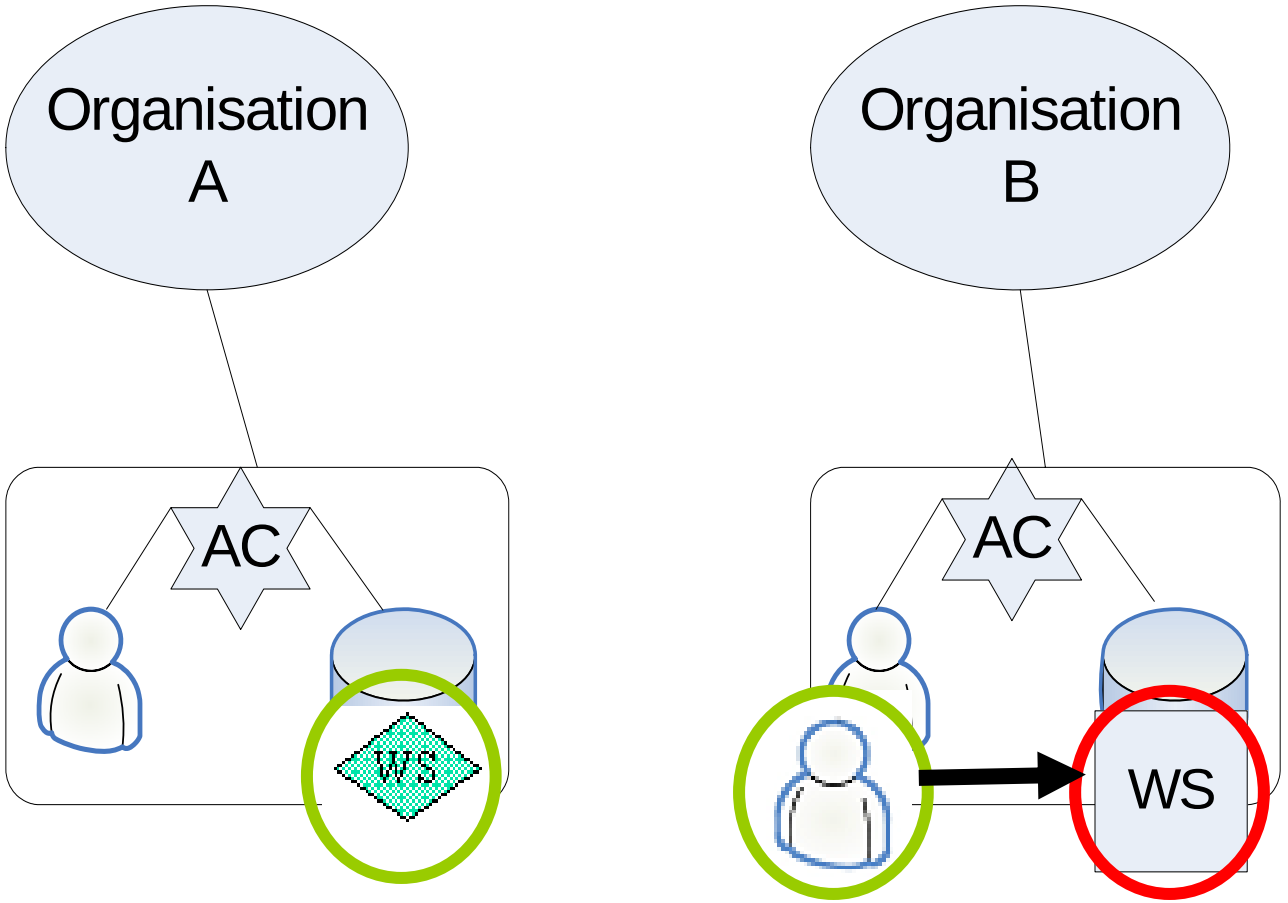
PolyOrBAC & WS



PolyOrBAC & WS



PolyOrBAC & WS



Summary on PolyOrBAC

- Each organization authenticates its users and manages its resources autonomously (local security policy).

- Interactions:
  - Through Web Services, with signed contracts + message logging (evidence)
  - The requesting organization is liable for its users
  - The providing organization is liable for the service: compliance with the contract

Contracts

- Negotiated before WS use
- Describe the WS: functions and parameters, expected quality of service, liability of each party, payment, penalties in case of failure/abuse, …

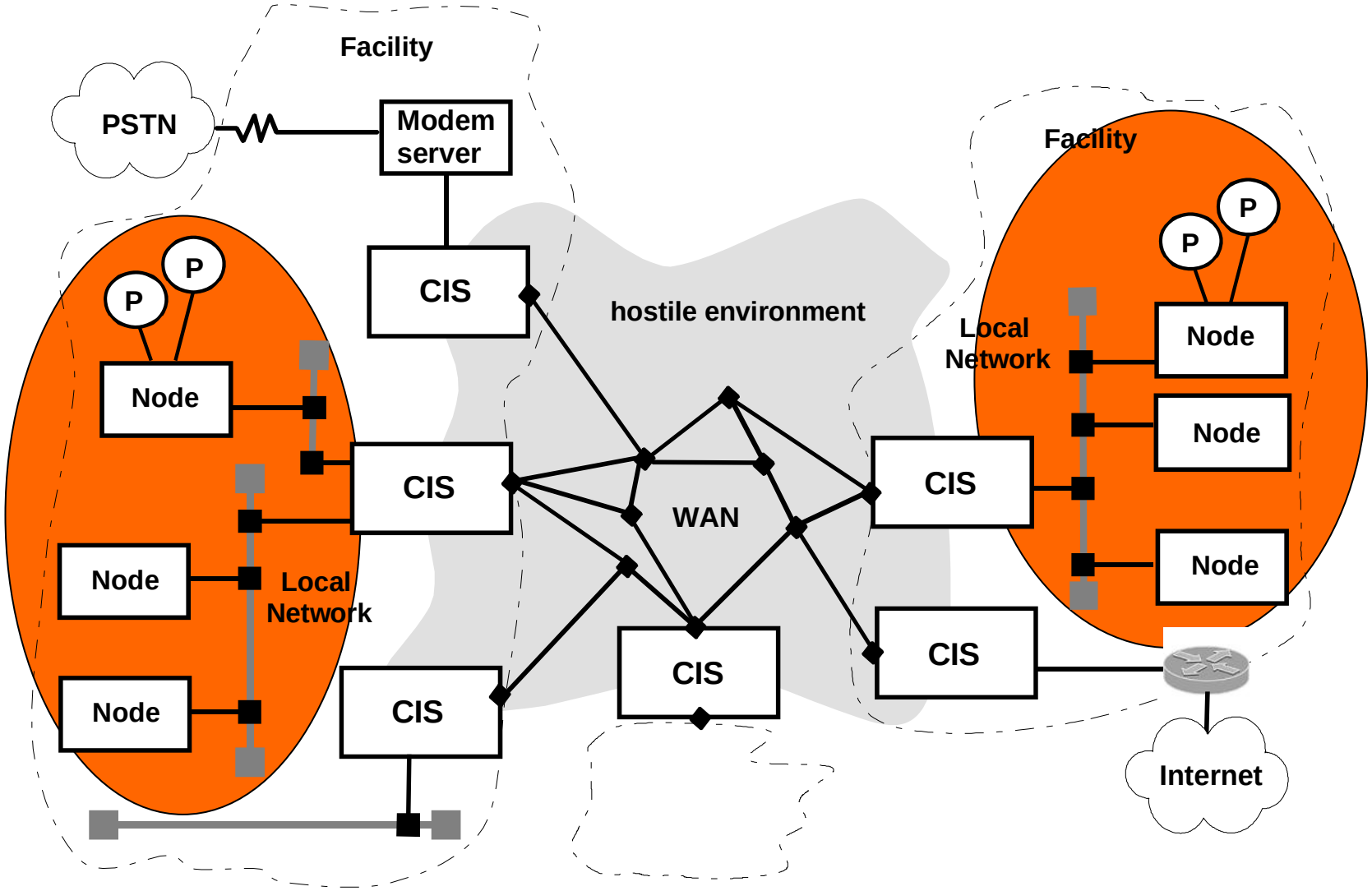
  + security rules (i.e., agreed security policy)
    - Permissions
    - Prohibitions
    - Obligations
- Verified at runtime + evidence collection
  - At the level of messages exchange

    --> 1 timed automaton on each side of the WS

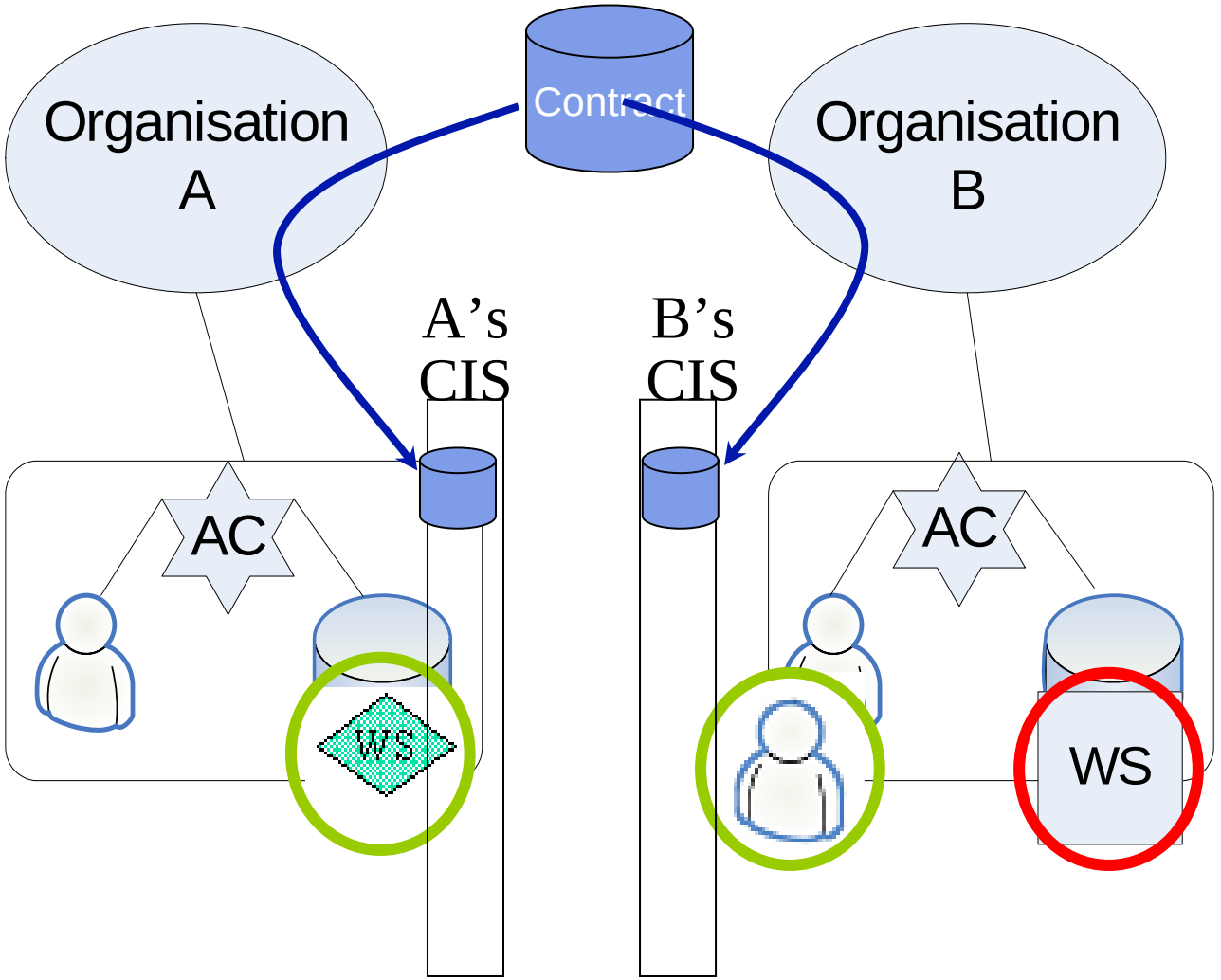
Run-time model checking

- Permissions = transitions between states, triggered by a valid WS message or by a local event
- Prohibitions
  - Implicit: no transition
  - Explicit: transitions to "failure states"
- Obligations ???
  - "Internal obligations" = transition automatically triggered by local events (guarded by time-out)
  - "External obligations" = those that must be realized by the other party, guarded by a local time-out: if a proof of achievement is not received before the time-out --> transition to an exception (obligation)

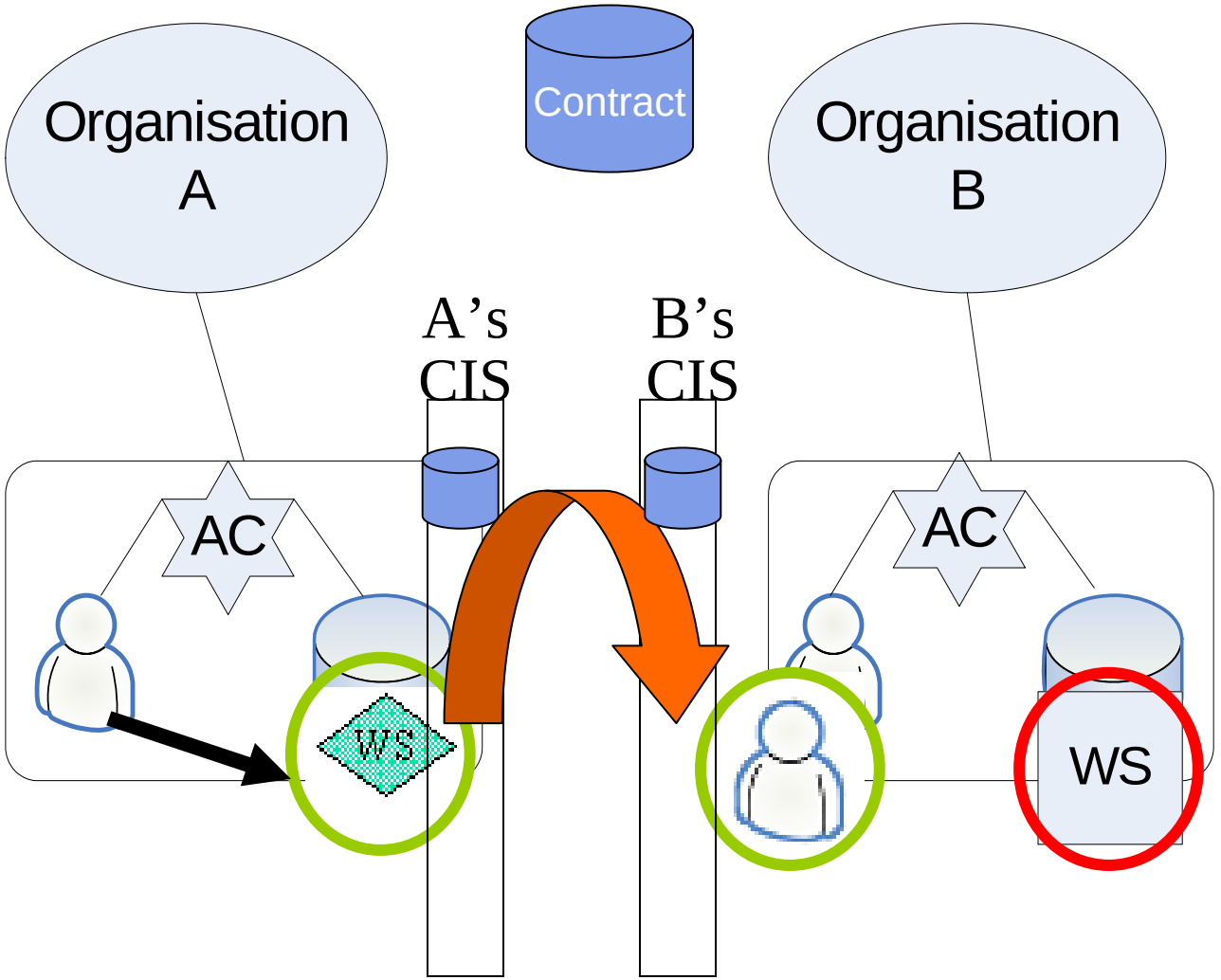
CRUTIAL Architecture



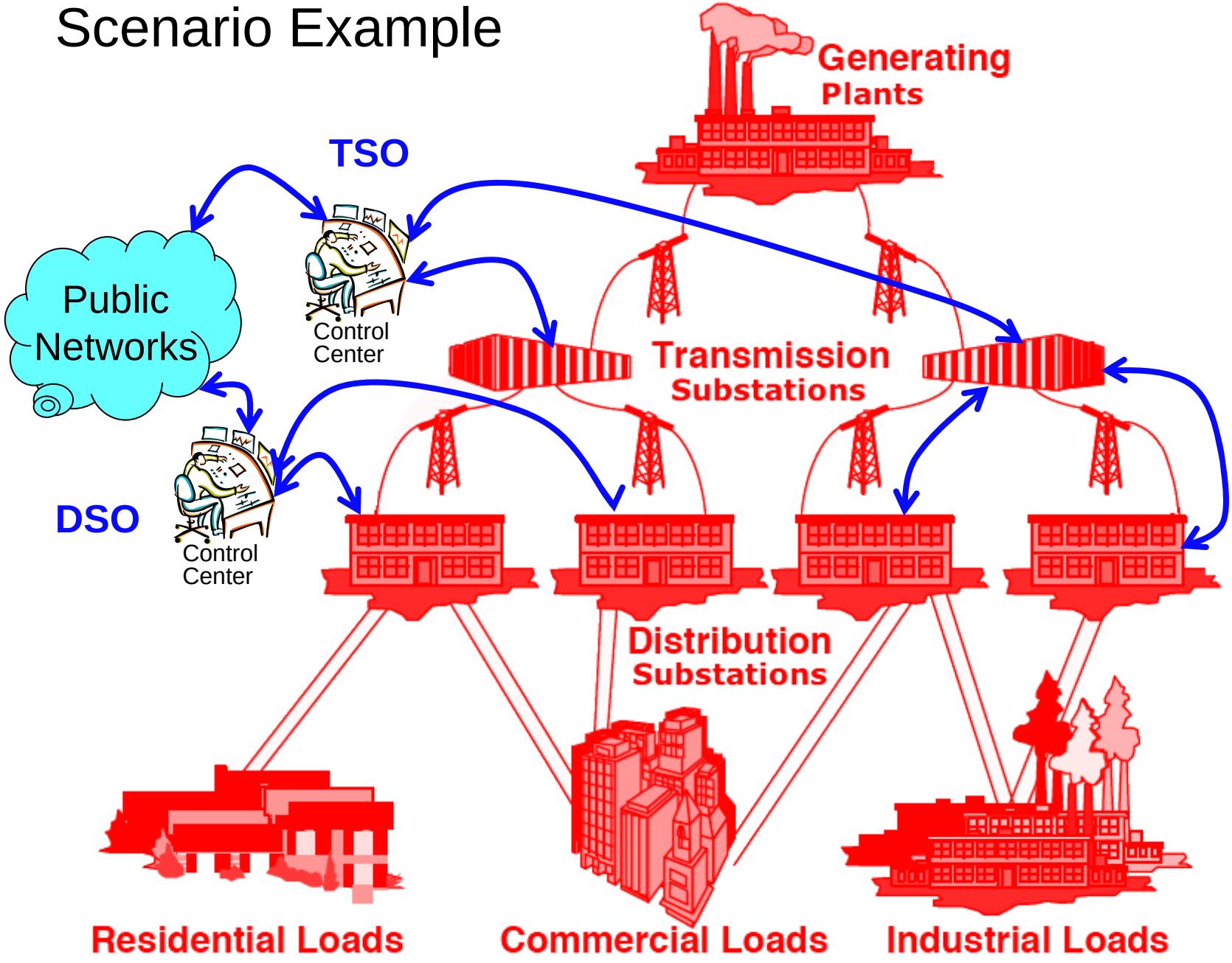
PolyOrBAC dans CRUTIAL

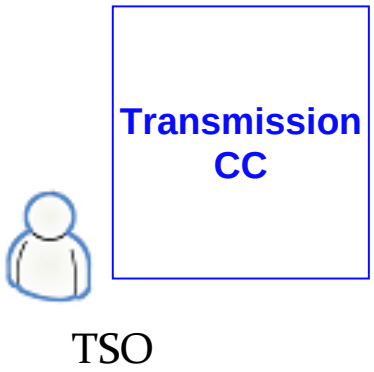


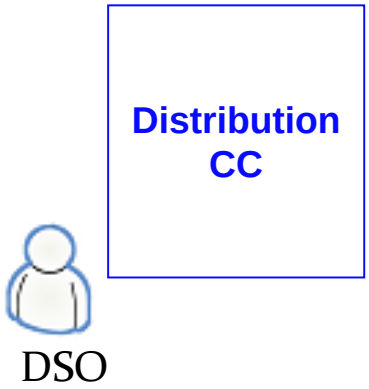
PolyOrBAC dans CRUTIAL



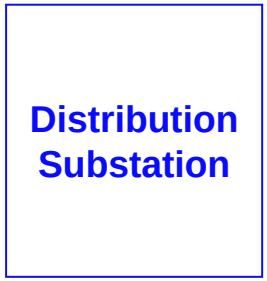
Scenario Example

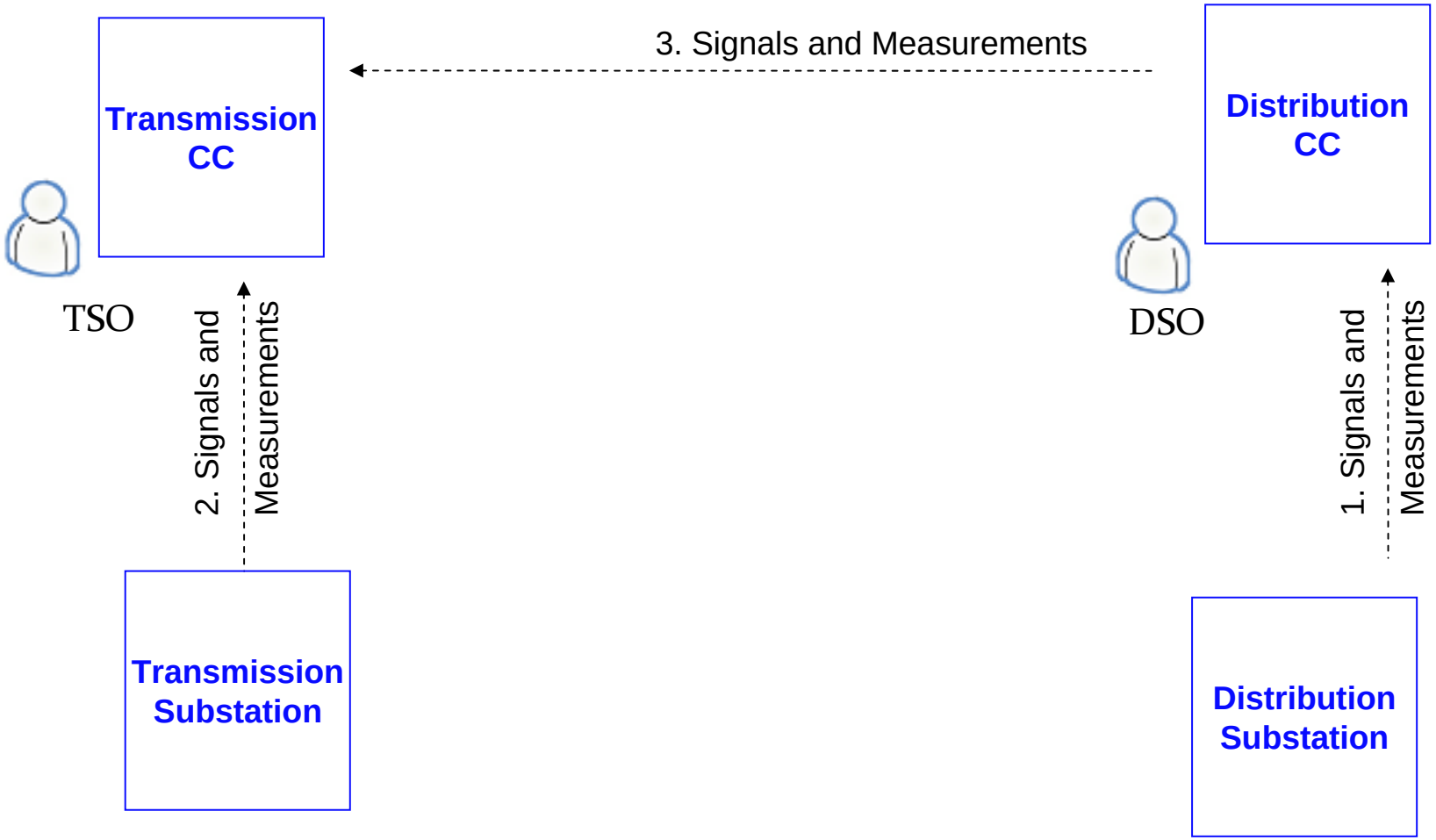



Transmission
CC
TSO

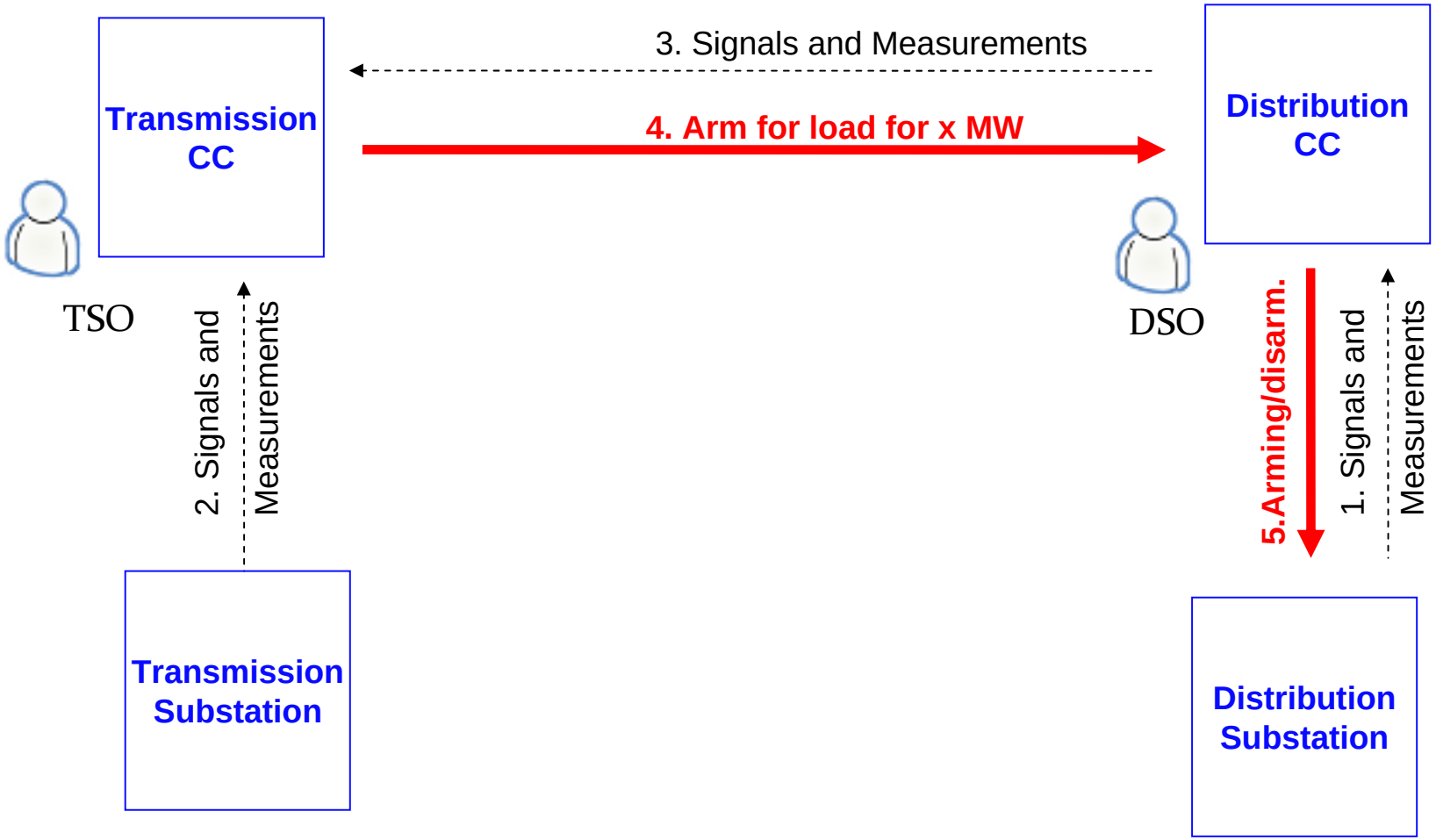

Distribution
CC
DSO

Transmission
Substation

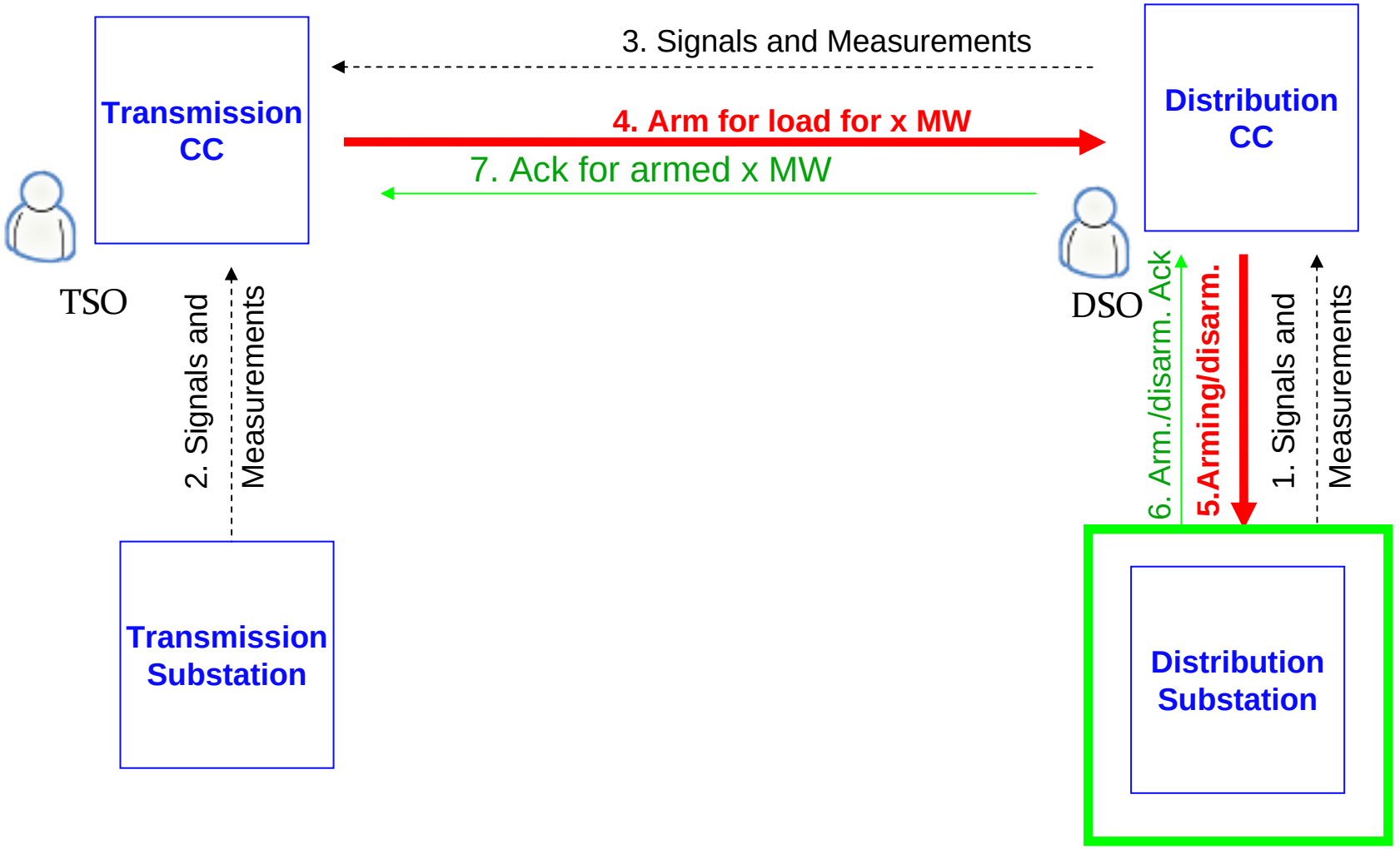

Distribution
Substation



Normal operation

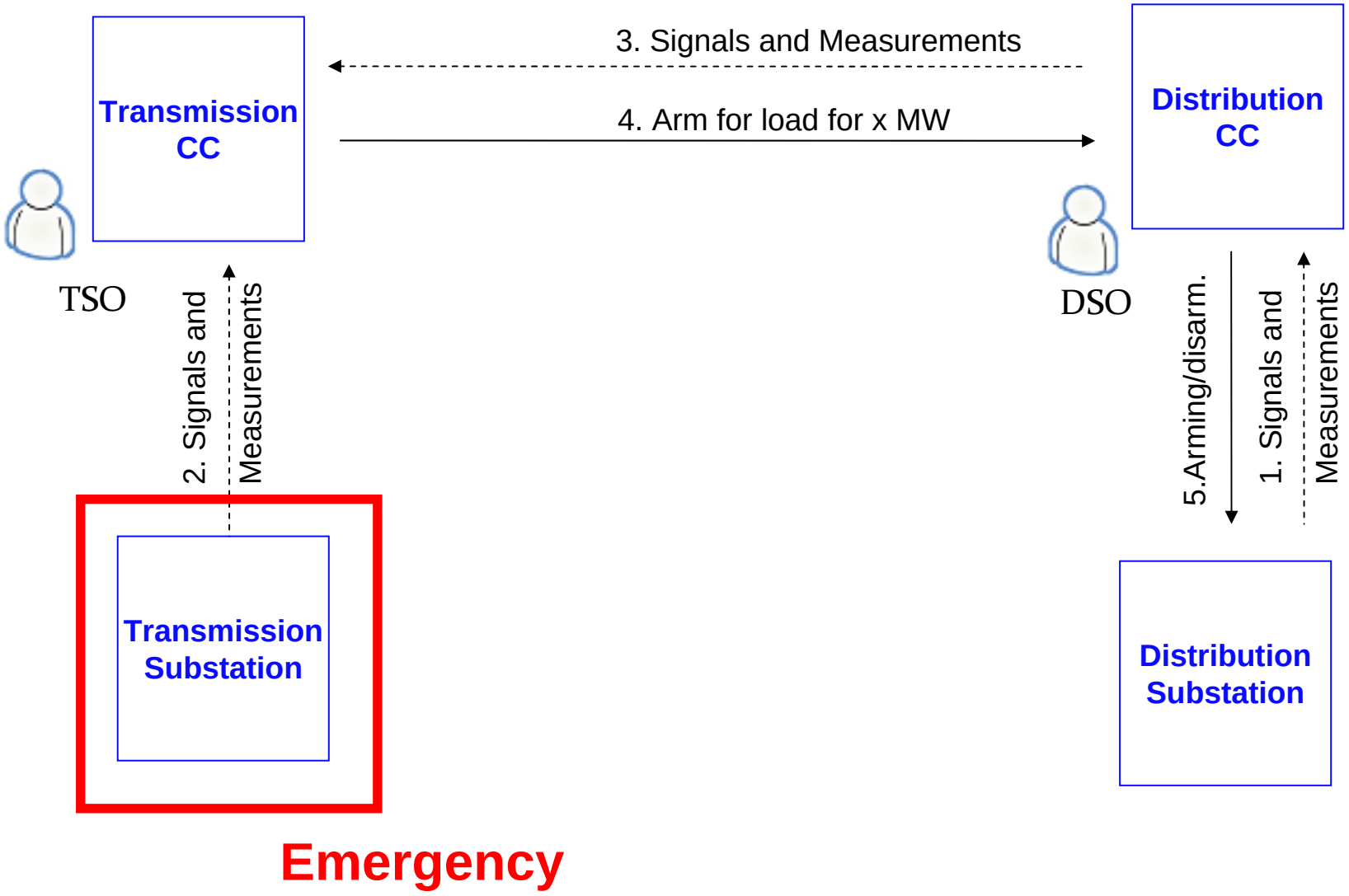


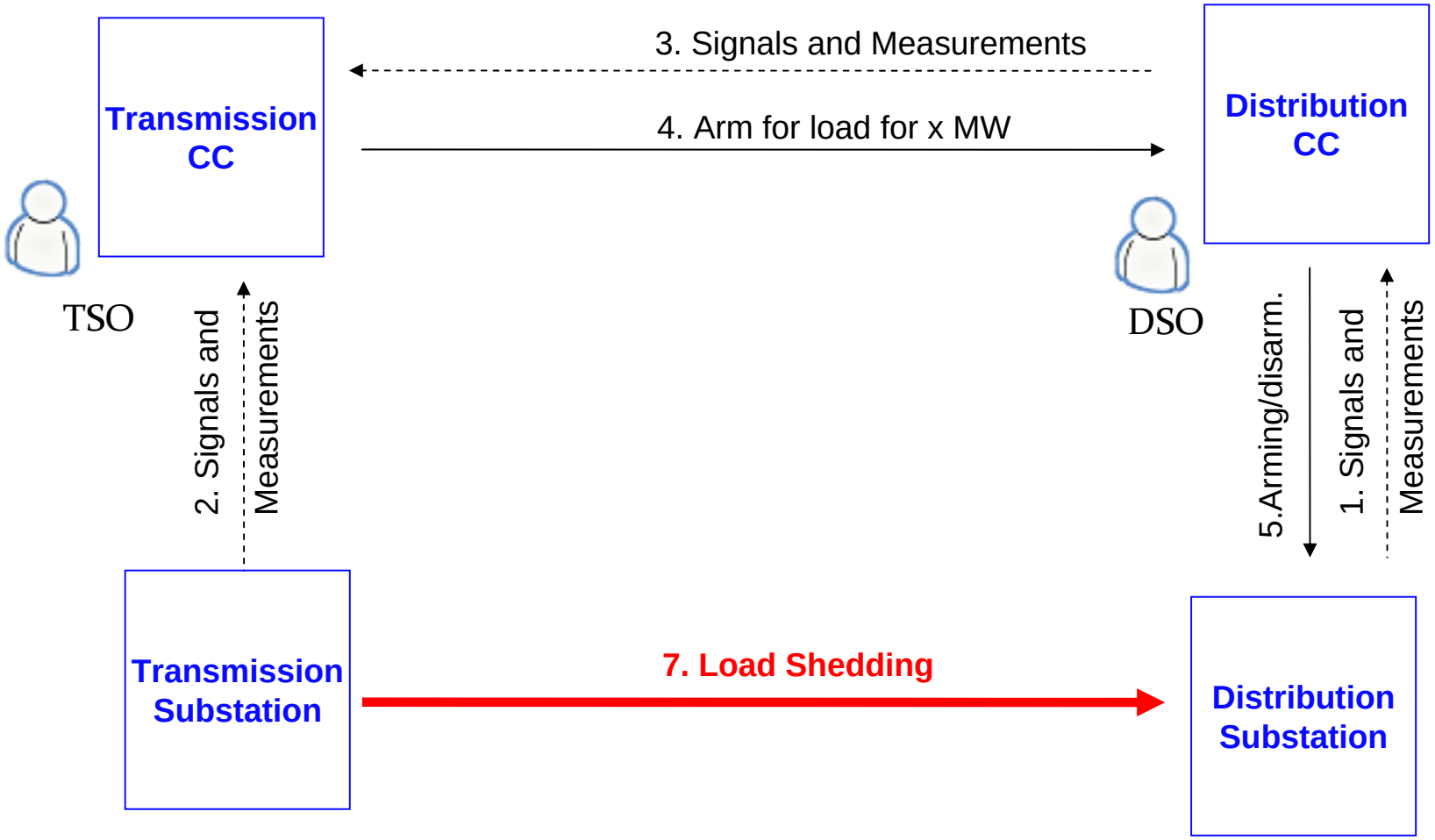
Prepare for possible load shedding



Ready for load shedding

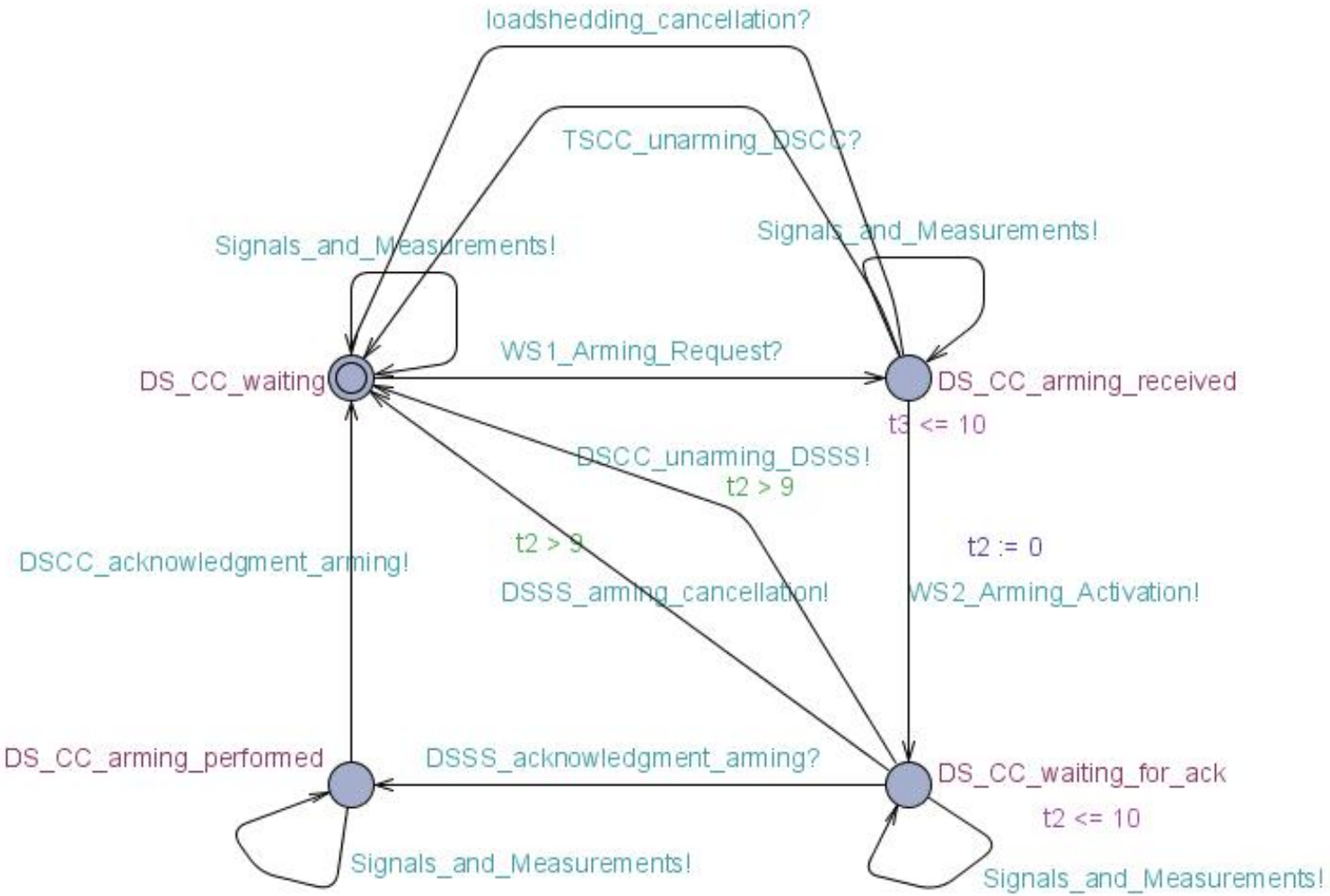
Note : 6 and 7 are facultative: the info can be transmitted by signals in 1&3
For 6 : disarming can be automatic


Transmission CC
3. Signals and Measurements
4. Arm for load for x MW
Distribution CC
TSO
DSO
2. Signals and Measurements
5.Arming/disarm.
1. Signals and Measurements
Transmission Substation
Distribution Substation
Emergency


Transmission CC
3. Signals and Measurements
4. Arm for load for x MW
Distribution CC
TSO
DSO
2. Signals and Measurements
5.Arming/disarm.
1. Signals and Measurements
Transmission Substation
7. Load Shedding
Distribution Substation

Example of automaton

Distribution System Control Center: arming/disarming DS Substations for load shedding



Conclusion

- General security model for inter-organization interactions
  - Each organization maintains its sovereignty on its assets (authentication, authorization) and is liable for its users
  - Interactions through Web Services, with controlled compliance with "contracts" verified at run-time
- An application scenario demonstration is currently developed in CRUTIAL